

ПРОБЛЕМЫ ОРГАНИЗАЦИИ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

В настоящее время актуальна проблема организации борьбы с киберпреступностью. В современном мире довольно часто совершаются преступления с помощью компьютерных технологий. Это обусловлено более широким распространением сети интернет, которая когда-то разрабатывалась лишь для того чтобы обеспечить более быстрый обмен данных в Пентагоне.

Чем больше человечество будет «переносить свою жизнь в электронный вариант», тем чаще будут совершаться преступления в сфере высоких технологий, а не те, к которым человечество привыкло за сотни лет, да и не только привыкло, но и разработало массу способов борьбы с ними. Среди преступлений, совершаемых с использованием компьютерных технологий, особенно возрастает численность в сфере экономики, в том числе:

- легализация доходов, полученных преступным путем с использованием компьютерных технологий;
- в банковской деятельности, в частности преступления с использованием электронных платежей;
- нарушение права интеллектуальной собственности на компьютерные программные продукты;
- промышленный, коммерческий шпионаж через глобальные сети телекоммуникации;
- недобросовестная экономическая конкуренция путем причинения вреда потерпевшим за блокирования или уничтожения их веб-сайтов или несанкционированное размещение на них с целью распространения через интернет дезинформации, порочащего деловую репутацию последних и т. д.

Конечно, вместе с развивающейся преступностью, повышается и подготовка сотрудников органов внутренних дел, в частности сотрудников отдела следственного комитета по борьбе с преступлениями в сфере высоких технологий. Так, каждую неделю компьютерные информационные узлы Пентагона подвергаются более 60 нападениям через средства электронной коммуникации, но защита, разработанная работниками службы компьютерной безопасности Пентагона, не только обнаруживает, но и предотвращает неправомерный доступ к системе.

Тенденция роста киберпреступности обусловлена следующими факторами:

- бурное развитие глобальной системы электронной телекоммуникации вроде интернет;
- присоединение к процессу формирования так называемой глобальной киберцивилизации новых стран через специальные национальные программы вроде: информатизации, развития информатики, информационного общества, постиндустриального общества, электронного общества и им подобных по смыслу;
- рост в структуре национальных экономик и международной экономике сектора торговли и предоставления услуг через электронные средства телекоммуникации.

Хотелось бы также привести в пример и ситуацию в Беларуси. Согласно статистике с сайта Министерства внутренних дел Республики Беларусь:

- 2004 год – 135 преступлений;
- 2005 год – 178 преступлений;
- 2006 год – 334 преступления;
- 2007 год – 996 преступлений;
- 2008 год – 1614 преступлений;
- 2009 год – 2154 преступления;
- 2010 год – 2514 преступлений;
- 2011 год – 2171 преступление;
- 2012 год – 2040 преступлений.

Анализируя вышесказанное, можно заметить, что до 2010 года киберпреступность росла, но с 2011 года пошла на спад. Также хотелось заметить, что, согласно статистике, с 2009 года совершались исключительно преступления: хищение путем использования компьютерной техники – ст. 212 Уголовного Кодекса Республики Беларусь (более 93 %) и преступления против информационной безопасности ст. 349–352, 354 (не более 6–7 %).

Так, согласно статистике за 2010–2012 гг. можно сказать, что тенденция роста киберпреступности прекратилась и даже пошла на убыль. Причинами этого могут быть:

- лучшая профессиональная подготовка кадров;
- более совершенная защита компьютерных сетей и т. п.

Тенденция убывания будет продолжаться, но хотелось бы внести предложения по ускорению этого процесса.

Во-первых, нанимать в правоохранительные органы больше молодых и креативных специалистов с техническим образованием и обеспечить им должную заработную плату, чтобы заинтересовать их работой в правоохранительных органах. Ведь молодой специалист-программист зарабатывает в Минске около 1500 долларов в месяц.

Во-вторых, использовать последние разработки в сфере высоких технологий и программного обеспечения, в том числе и зарубежные разработки.

В-третьих, достаточное финансовое обеспечение как правоохранительных органов, так и фундаментальных отечественных исследований в сфере борьбы и предотвращения киберпреступности.

Если полно следовать настоящей политике развития борьбы с киберпреступностью, а так же постоянно совершенствовать эту сферу, то в скором времени и эти преступления для правоохранительных органов станут обыденностью, как и способы борьбы с ней.